Unclassified Paper

NAVAL WAR COLLEGE
Newport, Rhode Island

Operational Protection of C4I

by

Gloria Dyer Mobery

Commander, United States Navy

A paper submitted to the faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

SIGNATURE:_____

05 March 1997

Paper directed by Captain George Jackson
Chairman, Joint Military Operations Department

REPORT DOCUMENTATION PAGE

1. **Report Security Classification:** UNCLASSIFIED

2. **Security Classification Authority:**

3. **Declassification/Downgrading Schedule:**

4. **Distribution/Availability of Report:** DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

5. **Name of Performing Organization:** JOINT MILITARY OPERATIONS DEPARTMENT

6. **Office Symbol:** C

7. **Address:** NAVAL WAR COLLEGE
686 CUSHING ROAD
NEWPORT, RI 02841-1207

8. **Title** (Include Security Classification): Operational Protection of C4I. Unclass

9. **Personal Authors:** Gloria Dyer Mobery, CDR, USN

10. **Type of Report:** FINAL

11. **Date of Report:** 07 February 1997

12. **Page Count:** 19

13. **Supplementary Notation:** A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. **Ten key words that relate to your paper:** Operational, security, command, control, computers, communications, intelligence, warfare, security, infrastructure.

15. **Abstract:**

The American way of war has been dependent upon information dominance in the battlefield for a long time. But the old ways of waging wars where the overwhelming force of the US provided a clear advantage may not be successful in fighting the wars of the future. This paper explores some of the problems associated with the protection of operational C4I assets in the current era and how CINCs can approach this planning issue.

As new technologies continue to emerge and are integrated into information systems that enhance decision making processes, the US national security functions are becoming more and more dependent on an information foundation which is embedded in larger national and international infrastructures. During the cold war, vast amounts of information was needed by the National Command Authority (NCA) to formulate broad policies and build national level strategic plans. But, with the cold war now over, regional military operational commanders such as Commanders in Chief (CINCs) and Joint Task Force (JTF) commanders need effective command and control information systems to help them plan and fight wars.

Military operations are now so dependent on national public and private information infrastructures that their information systems are a critical vulnerability. These vulnerabilities, and how they influence command and control must be better understood at the operational level. As systems become more integrated, they also become more vulnerable to, infiltration, penetration, and sabotage. Though information technology has proliferated at an astounding level, the development of technologies to protect these systems has not grown as quickly. Operational commanders should place greater emphasis on the protection of their systems through information security and counter-command and control techniques.

16. Distribution / Availability of Abstract:	Unclassified	Same As Rpt	DTIC Users
	X		

17. **Abstract Security Classification:** UNCLASSIFIED

18. **Name of Responsible Individual:** CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19. **Telephone:** 841-6461

20. **Office Symbol:** C

Abstract of

Operational Protection of C4I

The American way of war has been dependent upon information dominance in the battlefield for a long time. But the old ways of waging wars where the overwhelming force of the US provided a clear advantage may not be successful in fighting the wars of the future. This paper explores some of the problems associated with the protection of operational C4I assets in the current era and how CINCs can approach this planning issue.

As new technologies continue to emerge and are integrated into information systems that enhance decision making processes, the US national security functions are becoming more and more dependent on an information foundation which is embedded in larger national and international infrastructures. During the cold war, vast amounts of information was needed by the National Command Authority (NCA) to formulate broad policies and build national level strategic plans. But, with the cold war now over, regional military operational commanders such as Commanders in Chief (CINCs) and Joint Task Force (JTF) commanders need effective command and control information systems to help them plan and fight wars.

Military operations are now so dependent on national public and private information infrastructures that their information systems are a critical vulnerability. These vulnerabilities, and how they influence command and control must be better understood at the operational level. As systems become more integrated, they also become more vulnerable to, infiltration, penetration, and sabotage. Though information technology has proliferated at an astounding level, the development of technologies to protect these systems has not grown as quickly. Operational commanders should place greater emphasis on the protection of their systems through information security and counter-command and control techniques.

Operational Protection of C4I

"An effective C4 system crucial to successful planning, preparing, conducting, and sustaining major operations and campaigns, must be capable of providing rapid, reliable and secure information interchange throughout the chain of command."
Milan N. Vego

I. INTRODUCTION.

In the process of preparing for possible conflict, the operational commander must plan the execution of his campaign so that all operational level activities or *operational functions* are synchronized. During peacetime, the Commander in Chief (CINC) ensures these functions are incorporated into their plans and each plan is ready for combat operations. Of all operational functions (operational command and control, operational intelligence, movement and maneuver, operational fires, operational logistics, operational protection), the most important is command and control (C2) since it synthesizes the other functions together to produce the unity of effort needed to achieve strategic goals.[1] The C2 support system that integrates this whole process is the Command, Control, Computer, Communications and Intelligence or C4I information support system.[2]

C4I support systems are viewed as some of the most important resources the commander has available. Without timely and accurate details of the enemy's location, strength, and intentions, as well as knowledge of operational forces, the commander's ability to fight battles would be severely limited regardless of the effectiveness of either the weapons or troops. Since C4I assets are such critical assets, commanders are compelled to expend considerable efforts to ensure the theater's information systems are protected.

---

[1] JMO Dept., Operational Functions, Naval War College, 1995, p. 2
[2] Ibid. p.12

In the post cold war world, advancements in information technology are drastically changing the way the US conducts warfare. Modern military operations encompass integrated, joint maneuvers where instantaneous communications are essential to intricate command and control coordination. Information systems (IS) provide the operational commander with the advantage of observing the battlespace, analyzing events and directing forces. The tactical commander has the benefit of knowing the location and defenses of the target, enabling the commander to select the most effective weapon to launch an attack.[3] Improved communications and information sharing provide commanders with unprecedented quality and quantity of information which enhances their battlefield awareness. Although the opportunities for streamlining operations and improving efficiency are enormous, unfortunately, so are the risks associated with increased dependency on information systems.[4]

II. THESIS.

The increased efficiency in military operations brought about by advancements in information technology is considered by some to indicate another revolution in military affairs (RMA).[5] The difficulty with relying on information technology as the tool to provide us economies of time and force is incorporating the protection of these assets into operational plans.[6] As was the case with past RMAs, the failure of the operational commander to engage technological advancements using operational art planning techniques have defined the direction of the war.[7] Forward thinking CINCs will employ C4I systems using the tenets of operational design and planning to defend their assets.

---

[3] Defense Science Board Summer Study Task Force, "Information Architecture for the Battlefield," 1994, p.ES-1
[4] GAO Report, "Information Security-Computer Attacks at Department of Defense Pose Increasing Risks," 1996, p.3
[5] Ronald R. Fogleman and Sheila E. Widnall, "Cornerstones of Information Warfare," p.1
[6] Ernst K. Isensee, "Impacts on the Operational Commander in the Information Age," p.5
[7] Federal Advisory Committee, "Information Warfare-Legal, Regulatory, Policy and Organizational Considerations for Assurance," 1996, pp.1.1;2.5

This paper will explore some of the challenges CINCs face in trying to protect the information assets within their area of operations and ensuring reliable, secure information is received by tactical commanders. Discussions will focus on how and why the US military shifted from reliance on a closed, proprietary and relatively secure information system to dependence on a public, vulnerable information infrastructure. Finally, a review of some of the C4I areas most vulnerable to enemy penetration and potential damage that can be caused to operations will be presented with recommendations of what the operational commander must consider to protect these vital assets.

III. BACKGROUND.

A. What led the US military to become so reliant on an information infrastructure of public and private communications networks?

Initially, because of the sensitive nature of military operations, DOD information was processed and transmitted over extremely reliable and robust infrastructures to ensure the availability of critical information during crises. Information processing was primarily confined to mainframe systems operating in physically secure facilities and communications were conducted over a dedicated, redundant, and survivable communications structure known as the Defense Information Infrastructure (DII). As DOD began to stress joint operations and interoperability, and it saw the efficiencies, cost savings and overall successes achieved by private industries such as banking, retail and manufacturing, they automated and interconnected their operations. To further enhance production, defense industries soon turned to commercial networks to support their unclassified operations. As the military increased its dependence on commercial carriers and public networks, the results were improved response times, more economical

operations and overall better preparedness. Although operations improved, with the DII was no longer solely a defense infrastructure but part of a global information infrastructure (GII) with enormous interconnections, it was at increased risk of unauthorized access.[8] By relying on an infrastructure of public and private communications networks, the military is enabled to make more effective use of its forces. However, it is also left with inadequate protection.

With the cold war over and the threat of nuclear attack diminished, the National Command Authority's need for information to formulate broad policy and build national level strategic plans has been reduced also. Operational commanders are now the major users of information. In order to carry out assigned missions, CINCs must ensure information systems are protected from compromise. The challenge would not be so great if information was processed and transported over private military communications networks. But the reality is that 95% of the military communications are carried over public switched networks that are shared by individuals, governments and private corporations world-wide.[9] Without adequate protection mechanisms in place, sensitive military operations are susceptible now, more than ever, to invasion, sabotage, and/or corruption.

IV. VULNERABILITIES.

A. Why are C4I assets so vulnerable?.

Information warfare grew out of the defense department's desire for increased information integration. The US military relies heavily on information systems to support Department of Defense (DOD) functions such as payrolls, research data, intelligence, operational plans,

---

[8] Ronald Knecht and Ronald A. Gove, "The Information Warfare Challenges of a National Information Infrastructure," p.1

[9] "Unclassified Information Warfare Tutorial," Army War College, p. 1

procurement source selection data, health records, personnel records and weapons system maintenance records.[10] This in itself makes the US vulnerable to information warfare (IW) since the integrity of its information directly effects the success of military operations. But, tactical operations are also dependent on information systems. Major weapon systems are computer driven. Navigational assemblages require knowledge based guiding for precision operations and targeting, and commanders are increasingly more reliant on the intelligence provided by computers to provide them with dominant situational awareness.[11]

Today, to enhance our communication efforts and promote information sharing, almost all DOD voice and data telecommunications are provided by public networks owned by common carriers. Critical US information systems are tied to the private and commercial sector with routine uses of internet, INMARSAT, INTELSAT, and EURUSAT.[12] On a routine basis, defense uses the internet to exchange electronic mail, log on, download and upload files to and from remote sites around the world. International networks are used during military operations to gather and disseminate intelligence information and communicate with allies. In addition, commercial satellites are relied upon to provide back up communication support since public messages from regions of conflict can provide early warnings of developments sooner than traditional systems.[13]

Although DOD uses closed systems, routers, firewalls, and encryption to secure critical networks and message traffic, these secure transmissions are carried on the public switched network which are very vulnerable to IW attacks.[14] While current information technologies offer enormous substance to our warfighters, because of the inherent

---

[10] Ibid. p.6
[11] Defense Science Board Summer Study Task Force, "Information Architecture for the Battlefield," 1994, p.30
[12] Stefan Eisen, Jr. "Netware, Its not just for Hackers Anymore, NWC, 1995, p.5
[13] GAO, p.7

vulnerability of an electronic battlefield and the advantages offensive IW assaults offers adversaries, DOD can be sure it will be the target of an IW attack. The Defense Information Systems Agency (DISA) reports that in 1995 DOD may have been subjected to informational attacks over 250,000 times. This number is based on the steadily increasing number of reported attacks (53 in 1992, 115 in 1993, 255 in 1994, and 559 in 1995) and estimates that only about one in 150 attacks actually being reported.[15] With the exponential growth this problem has shown in recent years, the military is taking this situation very seriously.

Another reason defense is threatened by IW is because it acts as a force leveler. No other nation has the ability to challenge the US in a traditional force on force engagement. IW, however, has the capability to cause catastrophic breakdown of our information and communications infrastructure at very little cost and minor technical training. In the past, the resources of a nation was required to wage war. Today only a computer and modem is needed.[16] The National Security Agency has acknowledged that potential adversaries are compiling databases on DOD C4I systems and methods of attacking these systems. There are over 120 countries that have now, or are in the process of developing IS assault capabilities.[17]

IW is an attractive warfare option to adversaries because, not only is it effective, but it is difficult to trace. It therefore offers the perpetrator non-attributionary capabilities. For example, in 1994 two hackers took control of the laboratory support system of Rome Laboratory, the Air Force's premier command and control research facility in New York. They established links to foreign internet sites and stole sensitive tactical and artificial intelligence research. To avoid detection, they first

---

[14] The Army War College, Information Warfare Tutorial
[15] GAO, p.4
[16] Knecht, p.7
[17] GAO, p.5

accessed the lab computers via phone switches in South America, then through east and west coast commercial sites before attacking the Rome site. The hackers had access to the Lab computers for three days before they were detected. Had they opted to bring the network down upon initial intrusion, there would have been no way to detect them.[18] Understanding this, adversaries are now positioning themselves for a new kind of warfare within the information sphere where they can exert their will on the US.

B. Where are we most vulnerable to C4I attacks?

The image that comes to mind when you think of an attack on an information infrastructure is a human-induced, deliberate attack on a system. These attacks are by far the most common and most serious. Attackers have stolen, modified and destroyed data and software by installing "backdoor" files to allow unauthorized users access in the future, incorporating trojan horses in programs to provide authorized users with the ability to perform unauthorized functions, and introducing viruses which shut down entire systems denying services to users dependent on it for critical missions. These examples of malicious acts can cause detrimental harm such as erasing data or overloading a system. But not all damage is deliberate. Some of the disruptive forces that can corrupt portions of the infrastructure include natural events, mistakes in code, and technical failures. Lightning striking a critical network node could cause part of your network to go down or a power failure/electrical surge could cause loss of data.[19] Assaults can take the form of a physical attack on information components such as computers, communications, software, data, cable; information infrastructures; or logic attacks on data. No matter what type of attack, protection is still needed for all systems.

---

[18] Ibid. pp.12-14

[19] Chief, Information Warfare Division (J6K) Command, Information Warfare-Legal, Regulatory, Policy and Organizational Considerations for Assurance, 1995, p.2-6

Some very vulnerable areas are:

(1) Equipment. The miniaturization of technology provides forces with portable computers and communication systems to modify plans, tactics and strategies in real time. However portable technology also gives rise to problems of compromise. Placing equipment closer to the conflict provides adversaries access to vital US communications circuits and thus strategic and tactical information.[20]

(2) Communications. Communications between senior national or military leaders are critical to the execution of military operations. The military depends on the rapid transmission of satellites to facilitate communications, and because the US military relies so heavily on telecommunications for all levels of communications, there are many threats to these assets. IW attacks against satellite communications might hinder dialog by crippling satellites and satellite transmission stations, or jam selective radio transmission points. Attacks on stationary transmitters and relay stations should be expected from conventional and non-conventional sources. Though disruption of radio transmissions is not new, there are new techniques (or old techniques to new applications) which expand the spectrum of threats to communications systems.[21]

(3) Data manipulation. The possibility of false or misleading communications represent a significant threat to military operations. An example of this was during the Vietnam War when North Vietnamese radio operators impersonated soldiers to call in air strikes. Future attacks could take the form of one side modifying target data in another's computer. To avoid information uncertainties, it is critical that data

---

[20] Ibid. p. 2-62
[21] Ibid. 2-66

integrity be assured. Encryption, though good, does not ensure data integrity since introducing false data bits or modifying data elements in a data base can be done without reading the internal message. Individuals have also rerouted commercial lines. If used with military circuits, this technique could allow adversaries to request false attacks, delete correct data or add false data which could damage US interests.[22]

(4) Personnel. Much of the new systems architecture that will be used in future conflicts will most probably be shared by coalition members or alliance partners. When fighting as a technology dependent international organization using systems that bind US troops with allies, the militaries are dependent on information systems to maintain and deploy major weapon systems. These systems are vulnerable to attack by any number of adversaries who want to exert their will on allied forces by disrupting a coordinated campaign .[23] There are no guarantees this technology will not be shared with an adversary or used against the US in a future conflict. US forces must assume that shared information is compromised information.[24] If it is not a closed US military system, it must be expected to be vulnerable and subject to compromise.

Another area of concern is counterintelligence. International espionage has been redirected from the individual with access to classified materials to network administrators and computer servicemen. Defense computer systems are extremely complex and require constant maintenance to operate efficiently.[25] Unless service personnel are properly indoctrinated in operational security (OPSEC) measures, this is another potentially vulnerable area. The difficulty in keeping accurate audit trails of those who use the system and when they used it could provide a potential adversary with an offensive IW opportunity.

---

[22] Ibid. p. 2-67

[23] July Ryan, Gary Federici, and Tom Thorley, Information Support to Militay Operations in the Year 2000 and Beyond: Security Implications, 1993, p.17

[24] J6C, p. 2-63

Though not a specific vulnerability, the lack of doctrine addressing information issues could possibly be an area an adversary might exploit. The complexity of this new public/private operating environment has delayed the formulation any comprehensive information policy. While activities are underway at the national level to address political and strategic information protection issues, the operational commander needs to take immediate action to safeguard these assets.

V. OPERATIONAL PROTECTION.

A. Why should combatant commanders develop plans to protect C4I systems?

Improved information connectivity increases tension between operational security and effective planning. As system integration increases, operational security decreases. To counter decreases in security due to force integration and C4I vulnerabilities, the CINC must develop an operational protection strategy that provides information assurance for the theater of operations.

Currently, information technology is expanding faster than the understanding of inherent vulnerabilities. For this reason, combatant commanders have difficulty attempting to integrate defensive IW techniques into their operations. Operational planning for C4I protection will ultimately boil down to balancing the use of advanced technology with its potential risks. If CINCs plan to use information systems as a force multiplier, they must also be prepared to develop appropriate controls to ensure its availability, confidentiality and integrity. Unfortunately, most emphasis is placed on exploring the advantages of

---

[25] Ibid. p.5

technology; but without a C4I protection plan, the commander exposes his operations to unneeded risks.[26]

B. What is the CINCs role in the information age?

CINCs are tasked with conducting decisive regional operations. To carry out this mission, control over both the process and the output must be exerted.[27] In the information age, CINCs need to control information support systems and make sure information gets to where it is need to in a timely, protected manner. In the past information responsibilities were assigned to J-6 staffs. But responsibilities for information protection should not be centralized in support departments such as information resources or security. Information assurance is a front line operation which warrants the immediate attention of the commander. CINCs needs to understand that information assurance within the theater resides with them. Operational commanders must rely on their J6 staffs to keep up with what the information systems are and how they operate; but CINCs have to understand the limits of information and technology, and what can be done in the information world in order to define the requirements of the theater.[28]

C. Operational Planning for the Protection of C4I.

The CINC's goal for the protection of C4I assets should be to provide a theater infrastructure with built in resilience for its information and support resources. The first step in achieving this goal is to conduct a net assessment of assets. The net assessment will identify infrastructure functional dependencies, and when dependencies increase, as in times of conflict, maximum capacity of the infrastructure. It will also highlight discrepancies and equipment vulnerabilities in the

---

[26] Isensee, p.1
[27] Rice, p.3

infrastructure, and personnel, training, strategy and policy shortfalls.[29] Once functional dependencies are evaluated and deficiencies are identified, actions can be prioritized according to the theater goals. Since information proliferation is continuous, the CINC's assessment of priorities in the protection plan must be an iterative process.

Planning must include four levels: protection, detection, limitation, and recovery.[30]

PROTECTION. In the past, industries have protected their information assets by incorporating network encryption, network sniffers/ watchdogs, firewalls, routers, and authentication techniques into their information systems.[31] Although future strategies also seem to point in this direction, a severe "denial of service " assault by an adversary would render all these protective mechanisms useless. Encryption signals work fine for protecting the contents of information, but although an attack on an encryption devise may not expose the contents of information, it may stop information from flowing and consequently deny the user information.[32] At the very least information protection programs must include heightened technical and awareness training and advanced intrusion identification devises to be effective.

Although commercial companies are the driving force behind the information technology revolution, DOD needs to lead innovations in designing information protection products that address its specific needs. For example, in the civilian world, information protection is aimed at preventing access to information in a relatively static environment, using predictable communications, and with repeatable information needs. But, in addition to preventing access to information,

---

[28] Defense Science Board Summer Study Task Force, Information Architecture for the Battlefield, 1994, p.ES-2
[29] Ibid. p. 30
[30] Eisen, p.13
[31] J6C, 4-1

DOD has the additional concern of protecting and reconfiguring information systems in an unknown operating environment, and protecting access while authenticating users and user systems in a mobile climate with the very high possibility of network disruptions.[33]

DETECTION. Network System Administrators should be able to detect physical destruction or degradation of system performance and effects on information outputs. They must be equipped to know the status of the infrastructure on a global basis and be able to detect attacks that cause system failures. Recent tests by DISA revealed that 88% of the targeted computers could be penetrated, but only 4% of the successful penetrations were detected.[34] At the very least operational commanders need to know when their systems have been compromised and put contingency plans in place.

LIMITATION. Force training must limit its reliance on C4I systems. Units should be able to operate efficiently both with and without new technology. They must utilized the information provided by new technology, but should also be trained in how to operate at the grass roots level without it. Training has to include how to continue operations when information technology is rendered useless and should emphasize basic skills when the environment is not conducive to utilizing technology.[35]

The necessity to deal with a wide range of unanticipated crises that involve joint operations with questionable coalition partners, places additional requirements on DOD information systems. The ability to add new users, requirements and functionality to the system is a capability that should be further utilized.[36] Multi level security provides the ability to introduce new users to system without providing them overall access.

---

[32] Ibid. p.2-5
[33] Ibid. p.2-62
[34] GAO, p.3
[35] Task Force, p.45

Rather than installing new nodes and circuits every time the US is involved in a joint military operation with another nation, we allow them limited access to our information system. This does not entirely eliminate the problem of providing coalition members access to our system and possibly deciphering our strategies, but it does provide a means for increasing operational efficiencies among the joint fighting forces.

RECOVERY. Defense forces need to be skilled in rapid reconstruction. Network Administrators must be prepared to react effectively and efficiently if, and when a problem does occur, to diagnose, control, and recover quickly.[37] Past experience has shown that intruders have been able to crack many technologies using technical and non-technical means. Attackers may choose to disrupt rather than exploit systems in some cases. When going into combat, in addition to taking combat specialists, CINCs should be prepared to take an information specialist specially trained to troubleshoot systems at critical times.[38]

VI. CONCLUSION.

As the US military enters an age of IW, it should not only concern itself with the ever popular offensive IW, but it must be prepared to defend itself against attacks to the critical C4I infrastructure.

This paper presents some of the issues the CINC will be confronted with when designing defensive strategy against IW attacks. In addition to the technological protective measures, institutional changes need to be made in the training of users, system operators and system support personneltechnical training must keep pace with technology so users understand how equipment operates. Technicians must understand how

---

[36] Ibid. p.43
[37] J6C, p.2-63
[38] Eisen, p.4

to recover vita systems if they are damaged. Although CINCs have no direct control over the training of most of their forces until actual conflict, they are in a position to influence these training issues by stressing their needs.[39] Also, policy and information security training need to be constantly impressed upon users to keep security breeches to a minimum.

The challenge for operational commanders will be in not only protecting operations from the malicious attacks by potential adversaries, but also the unpredictable natural disruptions to the infrastructure, and external constraints to define needs based on assets that only belong to the CINC during times of conflicts or military operations other than war (MOOTW). But a CINC's most challenging task will be operating within a national component slowly working to develop doctrine for an extremely complex information systems environment. Though planning for the operational protection of C4I assets may seem inadequate in relation to the overall problem, as long as the level of consciousness and awareness of theater personnel increases, the security of C4I assets will benefit.

[39] Eisen, p.14

BIBLIOGRAPHY

JOINT SERVICE PUBLICATIONS

Joint Chiefs of Staff Publication 3-0, Doctrine for Joint Operation. Washington: 1995.

REPORTS

Report of the Defense Science Board Summer Study Task Force, Information Architecture for the Battlefield. a report from the Federal Advisory Committee, Washington DC, November 1994.

Julie Ryan, Gary Federici, and Tom Thorley, Information Support to Military Operations in the Year 2000 and Beyond: Security Implications. Alexandria, VA Center for Naval Analysis, November 1993.

Information Warfare - Legal, Regulatory, Policy and Organizational Considerations for Assurance. A research report for the Chief Information Warfare Division (J6K) Command, Control, Communications, and Computer Systems Directorate, Joint Staff, The Pentagon, July 1995.

General Accounting Office, Information Security - Computer Attacks at Department of Defense Pose Increasing Risks. Report to Congressional Requesters, Washington: May 1996.

BOOKS

Rice, M. A. and Sammes, A.J., Communications and Information Systems for Battlefield Command and Control. London, England: Brassey's Inc., 1989

ARTICLES

Izzo, Lawrence L. "The Center of Gravity is not an Achilles Heel." Military Review, January 1988

Owens, William A., "The Emerging System of Systems." Proceedings, May 1995, pp.35-39.

UNPUBLISHED PAPERS/ THESES

Carter, John W., "Information Management in a Joint Task Force" an unpublished thesis, Naval Postgraduate School, Monterey, Ca: June 1993.

Eisen, Stefan Jr., "Netwar, It's not just for Hackers Anymore" an unpublished paper, US Naval War College, Newport RI: June 1995.

Harley, Jeffrey A., "Information Technology and the Center of Gravity" an unpublished paper, US Naval War College, Newport RI: June 1996.

Isensee, Ernst K., "Impacts on the Operational Commander in the Information Age" an unpublished paper, US Naval War College, Newport RI: April 1995.

Joint Military Operations Department, "Battlespace Information, Command and Control (C2), Operational Intelligence, and Systems Integration" an unpublished paper, US Naval War College, Newport RI: November 1996.

Marr, Patrick M., "Information Warfare and the Operational Art" an unpublished paper, US Naval War College, Newport RI: June 1996.

Mosig, Joanne M., "Command, Control, Communications, Computers and Intelligence (C4I) in Revolution" an unpublished paper, US Naval War College, Newport RI: June 1996.

Vego, Milan N. "Operational Functions." an unpublished addendum to NWC 4026, US Naval War College, Newport RI: August 1995.

INTERNET ARTICLES

Dunlap, Charles J. Jr., "Sometimes the Dragon Wins", A paper presented at InfoWarCon IV, Brussels, May, 1996, <http://www.infowar.com/mil_c4i/dragon.html-ssi> (27 January 1997).

Fogleman, Ronald R. and Widnall, Sheila E. "Cornerstones of Information Warfare", <http://www.infowar.com/mil_c4ia.html-ssi> (03 January 1997).

Knetcht, Ronald and Gov, Ronald A., "The Information Warfare Challenges of a National Information Infrastructure", <http://www.infowar.com/mil_c4i/iwchall.html-ssi> (03 January 1997).

"Unclassified Information Warfare Tutorial", Army War College, Carlisle, PN, <http://CARLISLE-WWW.ARMY.MIL/usacs/iw/tutorial/execsum.html> (03 January 1997).

Wilson, Michael, "First Steps Toward a Defense", <http://www.infowar.com/mil_c4i/mil_c4id.html-ssi> (03 January 1997).